HSM(Hardware Security Module) 장비 사용시 유익한 점

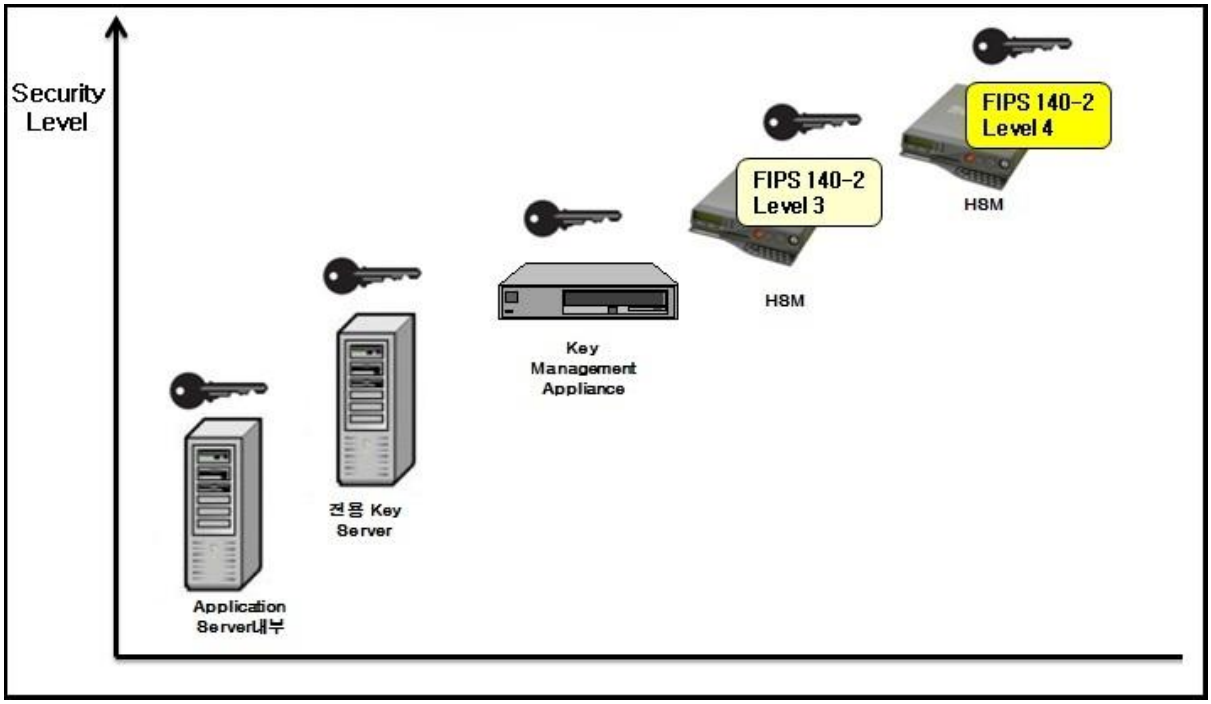
회사 기밀문서 보안의 핵심이 되는 암호키를 생성하고 보관하는 기능을 하는 전용 장비가 HSM(Hardware Security Module) 입니다만, 아직도 많은 기업에서 비용의 문제로 HSM 장비를 사용하고 있지 않은 것으로 알고 있습니다. 암호키가 유출됨으로 인해, 회사의 지적 자산이 유출되어 회사가 입는 손실은 너무나도 큽니다. HSM장비에 대한 투자 금액에 비하면 너무나도 적은 금액입니다. 비용을 떠나 회사의 존속에 영향을 미칠 수도 있다고 생각합니다. 국내에서 HSM장비를 사용하고 있는 곳도, 주 목적이 암호키의 안전한 보관 보다는 외부의 규제 사항 때문에(정부 또는 관계되는 회사의 요청 사항), 규제사항을 만족시키기 위해서라고 합니다. 또한 암호키 유출로 인해 심각한 사건이 발생하지 않았기 때문에 투자 필요성을 설득하기가 어렵다고 합니다(지금까지 발생한 데이터 유출 사건은 암호화 되지 않은 데이터가 유출되었기 때문에, 암호화에 대하여 초점이 맞추어져 있고, 암호키의 유출 가능성에 대한 고려는 심각하게 보지 않고 있다고 여겨집니다)

다시 한번 요약하면, 보안은 암호키에 의존하게 되고, 암호키는 안전하게 보관되어야 하므로, HSM 장비가 반드시 필요하다 라는 것입니다.

HSM 장비를 사용하지 않고 서버에서 암호키를 보관하게 되면, S/W방식이므로 서버내의 어딘 가에 파일 형태로 존재하게 됩니다(비록 여러번 복잡한 암호 방식으로 암호화 시켜 보관하였다 하더라도 하나의 파일이며 이것은 해독이 될 가능성이 높습니다), 또한 암호키를 사용한 암호연산을 서버에서 수행한다면, 서버의 메모리를 외부로 유출시키는 Heartbleed(2014년에 발견되어 패치되었음) 같은 Security Bug가 있다면, 암호키가 고스란히 유출이 되게 됩니다.

HSM 장비는 암호키를 안전하게 보관할 뿐만 아니라, 암호키를 사용한 암호연산도 HSM 장비 내에서 이루어 지도록 하는 기능을 제공합니다. 또한 HSM 장비로부터 암호키를 탈취하려는 시도가 있으면 스스로 저장된 암호키를 삭제하는 기능을 가지고 있습니다(어떠한 상황에서 암호키가 삭제되는 가에 따라 FIPS 140-2 Level 3 와 FIPS 140-2 Level 4 가 구분되어 집니다)

아래 도표는 보안레벨을 도식화 한 것입니다.

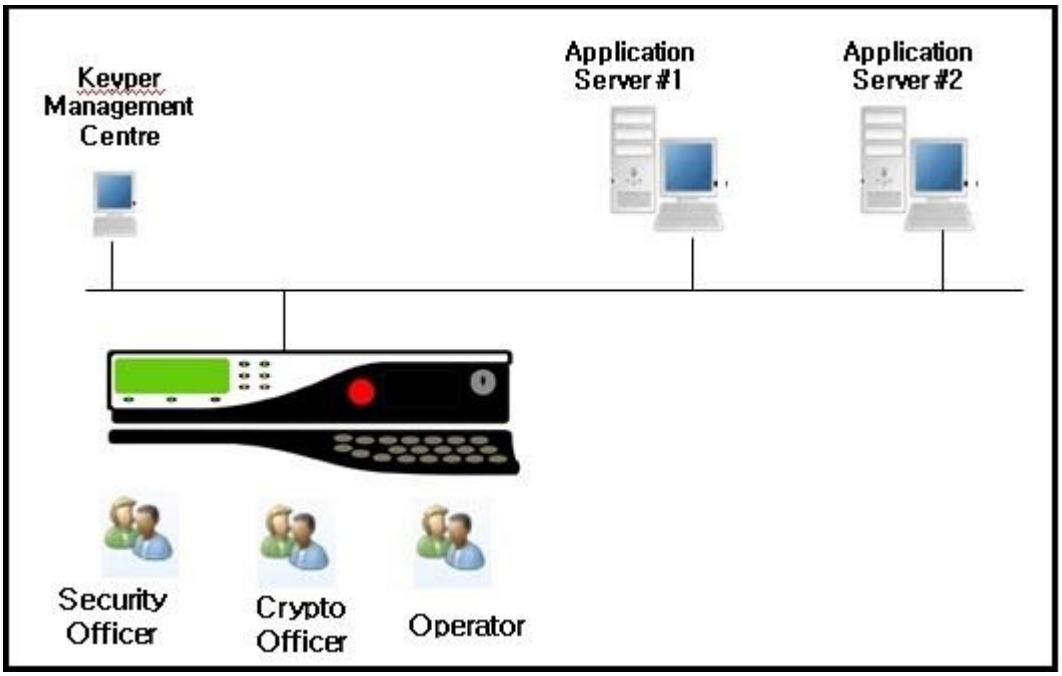


기능적인 측면 뿐만 아니라 관리적인 측면에서도 HSM 장비를 사용하는 유익한 장점들이 있습니다.

서버에서 암호키를 보관하고 있는 경우는 대개 서버를 관리하는 시스템팀 또는 네트워크 운영팀 또는 서버 운영팀에서 함께 관리를 하게 됩니다. 또는 암호키 관리자를 별도로 두더라도 서버 운영자도 암호키를 접근할 수 있게 됩니다(또한 서버를 접근할 수 있는 내부 공모자도 암호키를 접근할 수 있게 됩니다) . 하지만 HSM 장비를 사용하게 되면 독립된 전담 보안 팀에게 임호키 관리를 맡길 수 있습니다. 암호키를 접근할 수 있는 자는 HSM 장비에 의해서 인가된 관리자만 접근할 수 있게 됩니다. 이것이 HSM 장비 사용의 또 하나의 중요한 장점입니다. HSM 장비로 인해 관리자가 늘어나게 되지만, 이것이 바로 보안의 기본을 지키는 일입니다. 즉 HSM 장비 사용으로 인해 보안의 기본을 지킬 수 있게 된다는 의미입니다.

현재 HSM 장비의 보안 기능에 대한 표준은 FIPS 140-2 이지만 보안 기능을 더 보완하여 FIPS 140-3 표준을 준비 중에 있다고 합니다. 새로운 표준에서 권고하는 것은 HSM 장비 관리자를 3가지 그룹으로 나누라고 합니다(그룹이란 용어를 써는 이유는 혼자가 아니라 최소 2명 이상이 모여야지 만이 HSM 장비를 다룰 수 있게 한다는 의미입니다). "HSM장비 운영자", "HSM장비 관리자", "암호키 관리자"로 나누어 관리하라고 합니다.

HSM장비 운영자(Operator) : 장비의 On-Line/Off-Line 을 설정하는 자(전원 On/Off 가 아님)
⇨ On-Line이 되어야지만이 네트웍상에서 HSM에 Access할 수 있음
HSM장비 관리자(Security Officer) : HSM 장비의 정책 및 기능을 설정하는 자
암호키 관리자(Crypto Officer) : 암호키의 백업 및 복구를 포함한 암호키 자체에 대한 관리자



당사가 국내에 공급하는 HSM 장비인 KeyperPlus는 FIPS 140-2 Level 4 인증을 받은 장비이며, HSM 장비 관리자를 3가지 그룹(Operator, Security Officer, Crypto Officer)으로 나누어 지원합니다. High Security 요구하는 글로벌 기업 및 국가 기관들이 주 고객입니다. .

AEP-KoreaNet(www.kn.co.kr)